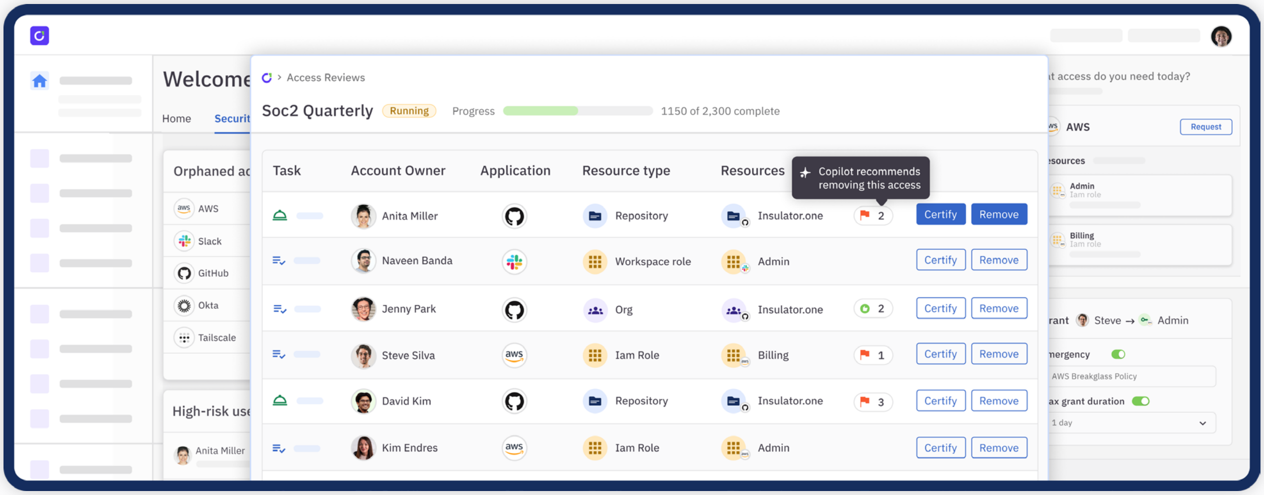
ConductorOne

15 Best Governance, Risk, And Compliance (GRC) Solutions for 2025

1. ConductorOne

ConductorOne is a cloud-based identity security and access governance platform that centralizes and automates access management across cloud applications and infrastructure.

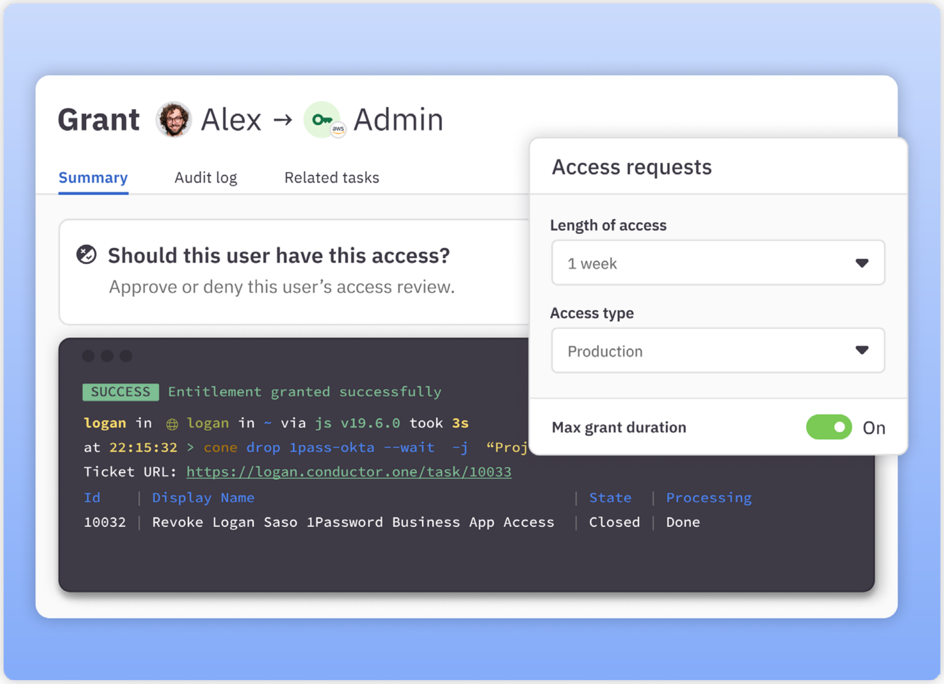


Soc2 Quarterly Running Progress 1150 of 2,300 complete

Task	Account Owner	Application	Resource type	Resources		
	Anita Miller		Repository	Insulator.one	⚑ 2	Certify Remove
	Naveen Banda		Workspace role	Admin		Certify Remove
	Jenny Park		Org	Insulator.one	● 2	Certify Remove
	Steve Silva	aws	Iam Role	Billing	⚑ 1	Certify Remove
	David Kim		Repository	Insulator.one	⚑ 3	Certify Remove
	Kim Endres	aws	Iam Role	Admin		Certify Remove

Copilot recommends removing this access

It implements least-privilege access principles through automated workflows for provisioning, deprovisioning, and periodic access reviews, while providing a self-service portal for access requests and approvals.



Should this user have this access?

Approve or deny this user’s access review.

```
SUCCESS Entitlement granted successfully
logan in  logan in ~ via js v19.6.0 took 3s
at 22:15:32 > cone drop 1pass-okta --wait  -j  “Proj
Ticket URL: https://logan.conductor.one/task/10033
Id     | Display Name                         | State  | Processing
10032  | Revoke Logan Saso 1Password Business App Access | Closed | Done
```

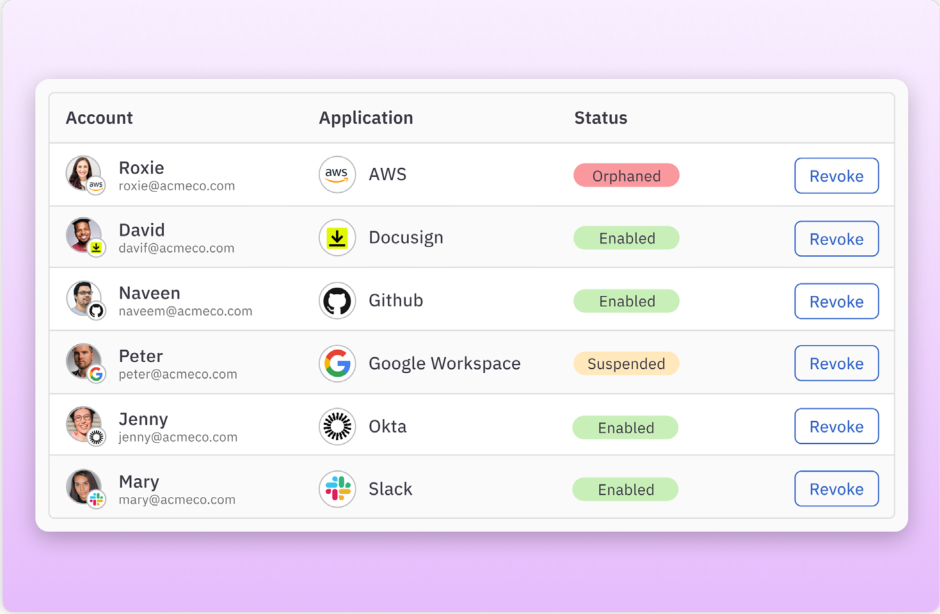
Access requests

Length of access: 1 week

Access type: Production

Max grant duration: On

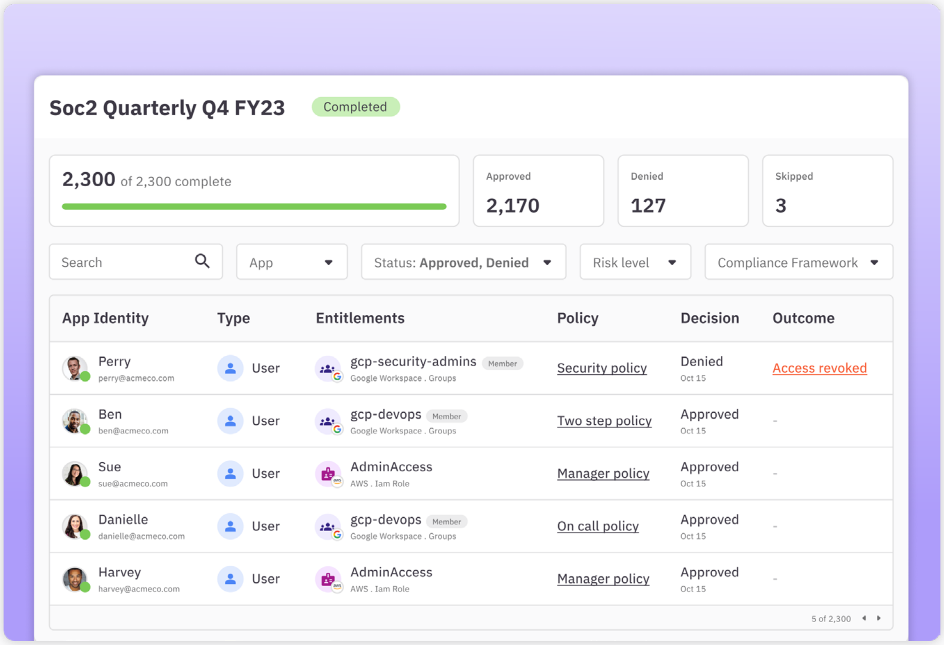
The platform integrates with both cloud services and on-premise systems to maintain a comprehensive inventory of user permissions and access patterns.



Account	Application	Status	
Roxie roxie@acmeco.com	AWS	Orphaned	Revoke
David davif@acmeco.com	Docusign	Enabled	Revoke
Naveen naveem@acmeco.com	Github	Enabled	Revoke
Peter peter@acmeco.com	Google Workspace	Suspended	Revoke
Jenny jenny@acmeco.com	Okta	Enabled	Revoke
Mary mary@acmeco.com	Slack	Enabled	Revoke

ConductorOne’s technical architecture leverages adaptive security policies that dynamically adjust based on contextual factors like location and device type, while its automation engine streamlines traditionally manual IAM workflows.

For organizations in regulated industries, ConductorOne provides granular audit trails and compliance reporting capabilities that track access patterns, policy changes, and approval workflows.



Soc2 Quarterly Q4 FY23 Completed

2,300 of 2,300 complete

Approved 2,170

Denied 127

Skipped 3

App Identity	Type	Entitlements	Policy	Decision	Outcome
Perry perry@acmeco.com	User	gcp-security-admins Member Google Workspace . Groups	Security policy	Denied Oct 15	Access revoked
Ben ben@acmeco.com	User	gcp-devops Member Google Workspace . Groups	Two step policy	Approved Oct 15	-
Sue sue@acmeco.com	User	AdminAccess AWS . Iam Role	Manager policy	Approved Oct 15	-
Danielle danielle@acmeco.com	User	gcp-devops Member Google Workspace . Groups	On call policy	Approved Oct 15	-
Harvey harvey@acmeco.com	User	AdminAccess AWS . Iam Role	Manager policy	Approved Oct 15	-

The system’s policy-based controls and detailed activity monitoring enable security teams to enforce least-privilege access at scale while maintaining visibility across complex IT environments.

Top Features

→ **Unified Access Request & Approval Portal.** Provides a centralized interface for users to request access to resources across all integrated systems. The portal displays available resources based on each user’s role and permissions, simplifying the request process. Approval workflows are also automated, allowing managers to review requests quickly while ensuring that requests are consistent with organizational access policies.

→ **Automated Access Reviews.** Automates periodic access review cycles, notifying managers to review and confirm each user’s access rights. This ensures compliance with regulatory requirements and minimizes the risk of privilege creep by maintaining only necessary permissions.

→ **Adaptive Access Policies.** Implements risk-based policies that allow or restrict access depending on real-time conditions, providing an additional layer of security that adapts to changing environments and reducing the likelihood of unauthorized access.

→ **Policy-Based Access Controls.** Allows administrators to define granular access policies based on specific roles, groups, or conditions. These policies automate access provisioning and deprovisioning, ensuring that permissions are assigned only when they meet predefined criteria. The policy engine supports fine-grained controls that allow organizations to enforce least-privilege access principles.

→ **Compliance and Audit Reporting.** Provides detailed logs of user activities, access requests, and approvals, enabling organizations to meet regulatory requirements for access management and maintain a clear audit trail. The platform generates customizable compliance reports that can be tailored to meet the needs of different frameworks, such as SOC 2, HIPAA, or GDPR.

What Makes ConductorOne Different?

→ **User-Friendly Access Request Interface.** With a straightforward, self-service interface, ConductorOne allows users to request and manage access without overburdening IT staff. This helps employees gain access when needed without complicated or delayed processes.

→ **Risk-Based Access Reviews.** By employing data-driven, risk-based assessments, ConductorOne prioritizes access reviews based on the level of risk, helping IT teams focus on high-impact areas first. This helps companies make informed decisions about which users have access to sensitive information and which areas need immediate review.

→ **Seamless Integration with Existing Tools.** ConductorOne offers robust Integrations with a wide range of cloud applications, IT infrastructure, and on-premise systems, including popular platforms like AWS, Google Cloud, Okta, and Microsoft Azure. This integration capability allows organizations to manage access permissions across various environments, ensuring that access governance policies are applied consistently throughout the IT ecosystem.

→ **Automated Access Control.** ConductorOne emphasizes a zero-touch automation model, which helps businesses reduce manual intervention but also ensures faster, more secure provisioning and deprovisioning of user access. This feature stands out in companies where complex workflows and multiple approval layers typically slow down access control.

→ **Fine-Grained Permissions Management.** ConductorOne enables precise control over permissions, allowing IT teams to define and enforce policies down to specific roles and tasks. This level of granularity helps organizations avoid over-provisioning, minimizing security risks associated with excessive permissions.

Why Do Companies Choose ConductorOne?

Picture this: You're managing hundreds of employees across different departments, each needing access to dozens of applications.

Without proper governance, it's a recipe for security nightmares – from forgotten access revocations to compliance violations. That's where ConductorOne steps in.

Companies choose ConductorOne for GRC because it automates the tedious parts of identity security while keeping them compliant.

But don't take it from us, listen to what RRCU's Information Security Officer, **Brandon Baker**, has to say.

> *"I didn't have easy options for integrating our old core—no APIs. So ConductorOne's ability to ingest on-prem application roles via CSV was really important for us."*

💡 **Read Case Study →** How RRCU Cut Risk With Automated User Access Reviews and Jit Access

Here's another one from **Ben Godard**, Director of Security Engineering, Spotnana.

> *"We needed a way to do self-service JIT that just worked. So someone could ask for access, the right person could approve that access, and the right amount of access could be granted for however long it was needed. Then it would go away. That was way more important than access reviews or all the other bells and whistles."*

💡 **Read Case Study ➜** How Spotnana Moved Critical Systems to Just-in-time Access to Secure Its Scaling Business

Some of our favorite people also had this to say:

→ *"The real strength behind ConductorOne is the ability to leverage its workflows against, at first glance, many disparate SaaS systems which may not have cohesive workflows out of the box."*
— **Tadayoshi H.** (Read full review).

→ *"Automating the end to end process from submission, approval and provisioning has significantly reduced our workload and a total game changer across the whole org."*
— **Anthony S.** (Read full review).

→ *"Going into implementation with ConductorOne, we set aside a full 3-4 weeks to work on setup. Once we got started, it was easier than we anticipated. We got our applications connected within the first week, set up our policies, and started running reviews in under a month."*
— **Ray M.** (Read full review).

Ready to Automate Your Identity Governance?

Discover How Leading Companies Use ConductorOne to Stay Secure and Compliant

Book a Demo

2. Riskonnect

Riskonnect is an integrated risk management (IRM) platform that helps organizations identify, monitor and manage various types of risks. This includes operational, strategic, compliance, cybersecurity, and ESG (environmental, social, and governance) risks.

Built on a cloud-based architecture, Riskonnect offers a single platform for managing risk across the enterprise, providing tools for incident tracking, claims management, compliance audits, and business continuity planning.

Riskonnects's centralized dashboard provides real-time insights into key risk indicators, and it supports proactive monitoring of risk trends. It also integrates with third-party data sources and tools, further enhancing its functionality by providing additional data streams for more comprehensive analysis.

Top Features

→ **Enterprise Risk Management (ERM).** Provides a centralized solution for identifying, assessing, and tracking risks across the organization. Users can score and prioritize risks based on their impact and likelihood, manage risk mitigation actions, and assign risk ownership.

→ **Incident and Claims Management.** Automates the claims lifecycle, from resolution to reporting, helping businesses manage insurance claims, track expenses, and analyze incident data for risk mitigation.

→ **Risk-Correlation Technology.** Enables organizations to anticipate, manage, and respond in real-time to strategic and operational risks across the extended enterprise.

→ **Business Continuity and Resilience.** The platform supports business impact analysis, contingency planning, and recovery strategies to help organizations maintain operations during and after critical events.

→ **Third-Party Risk Management.** Assesses and manages risks associated with vendors, suppliers, and partners.

Advantages

→ **Effective Risk & Safety Integration**. Combines risk and safety management in one location, enabling field users to gather information quickly and manage events efficiently [*].

→ **Strong Customization.** The platform offers extensive customization options and efficiently handles large volumes of records, providing unified access to claims, exposures, policies, and safety data across regions [*].

Disadvantages

→ **Overly Comprehensive Initial Setup.** The default setup ("vanilla package") includes more features than necessary for some users [*].

→ **Information Overload.** New users find the platform overwhelming at first due to the sheer amount of accessible information [*].

→ **Reporting Complexity.** Users find the reporting function less intuitive, often requiring additional help to navigate effectively [*].

Pricing

→ Contact Riskonnect for more information.

3. SAP GRC

SAP GRC is an integrated suite of tools that organizations use to manage risk, ensure compliance with regulations, and establish robust governance frameworks.

It integrates with SAP ERP and other SAP products, making it a powerful tool for organizations already leveraging SAP's ecosystem. The suite includes modules for risk management, audit management, access control, and business integrity screening, among others.

The platform automates regulatory compliance processes, helping businesses stay updated with current regulations and minimize manual efforts involved in audits and assessments.

For example, SAP GRC's real-time monitoring capabilities track policy violations, unusual access patterns, and other potential risks across SAP and non-SAP applications.

In addition, SAP GRC's modular structure enables companies to implement only the components they need, allowing for customized governance and compliance solutions that meet specific organizational requirements.

Top Features

→ **Access Control.** Automated user provisioning, enforces SoD rules, and monitors access requests for policy violations.

→ **Process Control.** It supports real-time control monitoring, control assessments, and policy violation tracking, helping organizations manage risks and maintain compliance with industry regulations. The feature also supports automated testing and documentation, making audit preparation faster and more efficient.

→ **Risk Management.** Allows users to define risk categories, set risk tolerance levels, and create action plans for risk mitigation.

→ **Fraud Management.** Employs predictive analytics and rule-based logic to identify anomalous patterns in transaction data, reducing the likelihood of financial and reputational losses.

Advantages

→ **3. Unified Process Control.** The platform delivers on its name by comprehensively managing company compliance, process control, risk management, and user access in one system [*].

→ **Advanced Integration Capabilities.** Easy-to-use interface provides comprehensive risk control and user access management, with ability to integrate with other systems like Oracle [*].

→ **Streamlined Authorization Management.** The ability to check authorization status and copy roles between users enhances efficiency, while providing comprehensive organizational risk assessment capabilities [*].

Disadvantages

→ **Performance Issues**. System suffers from significant slowdowns and delayed responses, requiring extensive RAM and space while increasing processing time [*].

→ **Role Discovery Challenges**. The system lacks intuitive role search functionality, making it difficult to identify needed roles without prior knowledge of the organization's specific role structure [*].

→ **Implementation Challenges**. Requires deep technical knowledge of SAP Basis and Security, while high costs and complexity make it unsuitable for smaller organizations [*].

Pricing

→ Contact SAP for more information.

4. Resolver

Resolver is a cloud-based risk management software designed to streamline and enhance the processes of incident management, risk assessment, internal audit, compliance, and IT risk management.

The platform provides organizations with a centralized solution to identify, evaluate, mitigate, and monitor risks— all in real time. Resolver integrates with existing systems and offers a flexible approach to GRC by allowing organizations to configure workflows, customize risk assessments, and automate reporting based on their specific needs.

In addition to risk and incident tracking, Resolver includes advanced analytics and data visualization tools, providing detailed insights into risk levels, compliance gaps, and control performance.
The platform's configurable dashboards and reporting capabilities enable organizations to keep stakeholders informed and ensure that decision-making is based on up-to-date risk intelligence.

Top Features

→ **Incident Management.** Offers automated workflows for reporting, escalation, investigation, and resolution, with features that allow organizations to log incident details, assign ownership, and track corrective actions.

→ **Compliance Management.** Automates compliance processes, tracks regulatory updates, and provides real-time compliance monitoring.

→ **Internal Audit Management.** Allows organizations to conduct risk-based audits, automate audit workflows, and track findings to resolution. It also includes collaboration capabilities, enabling teams to communicate audit findings and track corrective actions in real time.

→ **IT Risk Management.** Enables businesses to identify, assess, and mitigate vulnerabilities associated with IT systems and infrastructure

→ **Configurable Dashboards and Workflow Automation.** Allows users to view relevant metrics, while automated workflows streamline routine tasks, such as incident escalation, compliance monitoring, and audit tracking.

Advantages

→ **Portal Customization.** The platform offers extensive customization capabilities for templates and portals, allowing departments to tailor the system to their specific needs with easy reporting functionality [*].

→ **Seamless Implementation Process.** Despite the complexity of SaaS deployments, the platform offers smooth implementation with superior customer support and efficient security incident tracking [*].

→ **User-Friendly Interface & Integration.** Clean UI design with straightforward application creation and form building, enhanced by effective dashboards and easy API integration [*].

Disadvantages

→ **Configuration Complexity.** Despite unlimited customization options, users find it challenging to locate specific screen or field customization settings [*].

→ **Role & Report Management Issues.** Building and maintaining roles and reports proves more complex than basic form and workflow management [*].

→ **Complex Learning & Licensing.** Steep learning curve due to system's architecture, complicated by an unnecessarily complex licensing model [*].

Pricing

→ Contact Resolver for more information.

5. MetricStream

MetricStream is a leading provider of GRC solutions designed to help organizations streamline and automate their enterprise-wide GRC programs.

MetricStream's core offering is the ConnectedGRC suite, which provides a comprehensive set of applications to manage various aspects of GRC:

→ **BusinessGRC.** Focuses on enterprise and operational risk management, policy and compliance management, and third-party risk management.

→ **CyberGRC.** Addresses IT and cybersecurity risk management, IT compliance, and cyber policy management.

→ **ESGRC.** Supports environmental, social, and governance (ESG) initiatives by managing sustainability risks and compliance.

Top Features

→ **AppStudio.** A low-code development environment that allows users to configure and extend MetricStream applications to meet specific business requirements.

→ **Federated Data Model.** Provides a centralized data model with predefined relationships across risks, regulations, assets, controls, organizational entities, processes, and issues, ensuring a single source of truth for real-time, risk-aware decision-making.

→ **Continuous Control Monitoring (CCM).** Automates evidence collection at scale, offering total coverage compared to limited sampling in manual assessments, thereby enhancing efficiency and accuracy in compliance processes.

→ **Multi-Dimensional Organization Structure (MDOS).** Enables mapping of corporate hierarchy, geographies, and business units to risk and compliance information.

Advantages

→ **Flexible Risk Assessment.** Provides excellent IT risk management visibility with adaptable scoring systems and easy integration of company-specific factors [*].

→ **Professional Integration Support.** Qualified professional team effectively translates client needs into easily implementable and integrated models [*].

→ **Advanced Threat Management.** Platform enables companies to move from traditional risk management to threat-driven decision-making, leveraging real-time cyber intelligence for remediation actions [*].

Disadvantages

→ **Complex Licensing Structure.** Per-app licensing model increases costs for cross-app business cases, while system complexity creates initial understanding challenges [*].

→ **Limited Customization Options.** Lacks ability to deactivate unnecessary fields and needs improved cross-module data integration for metric-oriented dashboarding [*].

→ **Integration Challenges.** Complex integration processes with internal tools lead to delayed build times despite available system connections [*].

Pricing

→ Contact MetricStream for more information.

6. AuditBoard

AuditBoard is a cloud-based platform specializing in audit, risk, and compliance management. It provides a centralized platform where internal audit, risk, and compliance teams can manage their activities collaboratively. This includes tools for end-to-end audit management, from planning and fieldwork to reporting and follow-up.

AuditBoard also features a SOX compliance solution, simplifying the management of controls testing, documentation, and reporting, while its risk management tools help organizations identify, assess, and monitor risks in real time.

AuditBoard is particularly beneficial for medium to large enterprises and industries with stringent compliance requirements, such as finance, healthcare, and manufacturing.

Top Features

→ **SOXHUB:** A specialized feature for managing Sarbanes-Oxley (SOX) compliance. It streamlines the process of documenting, testing, and certifying internal controls over financial reporting. It offers features such as control mapping, testing workflows, and certification processes.

→ **OpsAudit.** Focuses on operational audits, providing tools to plan, execute, and report on audits across various business processes.

→ **AuditBoard AI.** Leverages artificial intelligence, including generative AI, machine learning, and natural language processing, to automate workflows, surface key insights, and manage risks more efficiently.

→ **CrossComply**. A compliance management solution that automates evidence collection, integrates assessment processes, and provides a centralized location for managing compliance controls.

→ **RiskOversight.** Enables organizations to visualize and address risks across the enterprise by mapping complex parent/child relationships within risk categories and aggregating risk scores for a comprehensive view of risk health.

Advantages

→ **Enhanced Efficiency Tools.** Significantly improves audit efficiency through user-friendly interface and seamless handling of complex tasks like planning, risk assessments, and tracking [*].

→ **Comprehensive Support System.** Offers extensive support through regular webinars, office hours, help center resources, and an active community, alongside customizable modules for team-specific needs [*].

→ **Strong Implementation Impact.** Delivers noticeable company-wide improvements, especially in issue action plan responsiveness, with continuous process enhancement through regular updates [*].

Disadvantages

→ **Workflow Limitations.** Lacks time-saving features like work step copying, requiring manual creation of repetitive elements during field work [*].

→ **Inconsistent Feature Implementation.** Cross-program changes and patches can create confusion and inefficiencies across different modules [*].

→ **Complex Permission Structure.** Administrator-level permission management is complicated, requiring careful understanding of teams versus roles, while frequent feature releases can confuse users [*].

Pricing

→ Contact AuditBoard for more information.

7. SAI360

SAI360 provides a centralized platform for managing GRC activities, allowing organizations to streamline risk assessments, automate compliance monitoring, manage audits, and track third-party risk.

Its integrated approach helps organizations identify, assess, and mitigate risks in real-time while ensuring compliance with industry regulations and internal policies.

SAI360's configurable dashboards and analytics tools provide detailed insights into risk exposure, compliance status, audit findings, and incident data, enabling stakeholders to make informed decisions and improve GRC performance.

The platform also supports health, safety, and environment (HSE) management, helping organizations meet workplace safety standards, track incidents, and promote a safe and compliant work environment.

Top Features

- **Smart EHS&S.** Integrates safety and sustainability features, enabling organizations to manage contractor safety and evaluate performance effectively.
- **Operational Risk and Vendor Intelligence Dashboards.** Provides real-time insights into vendor performance, including issue resolution speed, incident tracking, contract renewals, and operational resilience.
- **Solution Configurability.** Features an extensible data model with configurable user interfaces, forms, fields, and relationships, allowing organizations to tailor solutions to their specific needs.
- **Learning and Best Practice Content.** Includes preloaded frameworks, control libraries, and regulatory content, along with values-based ethics and compliance learning materials to support organizational training and development.
- **AI Audit Assistant.** Utilizes advanced artificial intelligence to automate the processing and analysis of audit evidence, accelerating workflows and ensuring accuracy without manual intervention.

Advantages

- **Customizable Modules.** Enables building separate workflows within each module to precisely meet organizational needs [*].
- **Efficient Audit Management.** Streamlines RAC audits with easy data collection and reporting capabilities [*].
- **Strong Compliance Features.** Particularly effective in cloud environment compliance, with organized policy management and robust audit trail capabilities [*].

Disadvantages

- **Configuration Tool Limitations**. Lacks advanced tools for environment migration, user rights management, and data archiving, with limited Microsoft Office integration for on-premises clients [*].
- **Complex Module Understanding.** Users face difficulties understanding module builds and maximizing application potential due to complicated structure [*].
- **Contract Process Issues.** Initial contract process is cumbersome and problematic. In fact, a user complained of the lengthy back and forth process to get an NDA [*].

Pricing

→ Contact SAI360 for more information.

8. Onspring

Onspring is a no-code GRC software built on a flexible data model that enables custom application development for risk management, compliance, audit, and vendor management processes. The system's core architecture supports dynamic risk scoring, automated workflows, and configurable assessment frameworks without requiring programming knowledge.

Onspring also handles automated control testing, compliance monitoring with rule-based alerts, incident tracking with SLA management, and centralized document management with version control.

The platform also provides real-time reporting capabilities, SAML 2.0 authentication, and RESTful APIs for enterprise system integrations with tools like SAP, ServiceNow, and Jira.

Each module can be customized through drag-and-drop interfaces while maintaining data relationships and audit trails across the platform.

Top Features

→ **Integrated Risk Management.** Offers a centralized risk register to document and assess risks across the organization. It supports automated risk assessments, prioritization of risk analyses, and tracking of mitigation efforts.

→ **Compliance Management Automation.** Integrates control libraries and maps them to various regulations and frameworks, such as ISO, NIST, and CMMC. It automates compliance testing, issue management, and reporting to ensure adherence to regulatory requirements.

→ **Policy Management.** Includes a comprehensive policy portal for authoring, distributing, and managing policies. It facilitates policy attestations, exception tracking, and ensures that employees have access to the latest policies and procedures.

→ **Third-Party Risk Management.** helps organizations assess, tier, and track vendors by integrating criticality ratings from cyber and financial monitoring services. It enables onboarding of new vendors, management of assessments, and tracking of mitigations to minimize third-party risks.

→ **Continuity and Recovery Planning.** Assists in linking Business Impact Analysis (BIAs), automating testing, and activating continuity plans.

Advantages

→ **Scalable Functionality.** Offers better flexibility in complexity levels, supporting various daily processes from simple to complex operations [*].

→ **Exceptional Customization & Support.** Platform offers high customizability without IT dependency, backed by comprehensive training options and dedicated customer support representatives [*].

→ **Strong Integration Features.** Excels in connecting and integrating applications, with simple app creation and Excel compatibility [*].

Disadvantages

→ **Change Management Challenges.** Difficulty in locating and accessing change options, combined with expensive user licensing [*].

→ **Cross-Platform Data Access Issues**. Limited references between apps create challenges in accessing data across different platform sections [*].

→ **System Timeout & Delegation Problems**. Issues with timeout function reliability and delegation system requiring manual email updates rather than automatic recipient adjustments [*].

Pricing

→ Contact Onspring for more information.

9. IBM OpenPages

IBM OpenPages is an AI-powered GRC platform that provides integrated risk management, regulatory compliance, operational resilience, and business continuity capabilities.

It leverages IBM Watson AI capabilities to operationalize risk management and regulatory compliance across all three lines of business, with zero end-user training required.

The system enables quick automation GRC processes within minutes through agile implementation workflows. Its core functionality includes embedded guidance for real-time user support, automated regulatory change management, and centralized risk monitoring.

Top Features

→ **External Loss Events Integration.** Integrates with IBM FIRST Risk Case Studies, enabling users to consider industry-wide loss events and incorporate them into scenario analyses, assessments, and risk management, ensuring a broader risk perspective.

→ **Scenario Analysis.** Leverages relevant system data to inform scenario workshops and identify scenarios requiring additional risk treatment, promoting proactive risk management.

→ **GRC Calculations.** Automatically assigns values to fields based on object creation, updates, or associations, streamlining governance, risk, and compliance processes with precision.

→ **Watson Language Translator Integration.** Detects and translates over 50 languages, ensuring content accessibility across language preferences set within OpenPages.

→ **IBM Cloud Pak for Data Cartridge.** Provides flexible deployment across any cloud platform, integrating IBM and partner capabilities to accelerate AI-driven insights and GRC processes.

→ **IBM Watsonx Assistant.** A virtual assistant offering 24/7 support for OpenPages users, answering common questions interactively and providing natural language search and direct links to specific pages or documents.

Advantages

- → **Powerful Analysis Capabilities.** Effectively uses machine learning algorithms to understand context and identify patterns in large datasets with high precision [*].
- → **Robust Data Processing.** Provides high-quality text analytics with metadata extraction capabilities and cloud deployment options for handling large data volumes [*].
- → **User-Friendly Implementation.** Requires minimal special training with comprehensive documentation support, eliminating need for dedicated data engineers [*].

Disadvantages

- → **Cost Barriers.** High pricing structure creates accessibility challenges for small businesses and individuals despite flexible pricing factors [*].
- → **Data Security Concerns.** Cloud storage raises security concerns, with challenging tool integration and extensive training data requirements [*].
- → **Complex Reporting Tools.** Cognos integration proves difficult for beginners, while access management features are powerful but overly complex [*].
- → **Accuracy Inconsistencies.** Constrained knowledge base can lead to inaccurate results, particularly challenging given the high price point [*].

Pricing

- → Contact IBM for more information.

10. LogicGate Risk Cloud

LogicGate Risk Cloud is another highly configurable no-code GRC platform that enables organizations to build and scale risk and compliance processes tailored to their unique needs.

Risk Cloud combines modular applications with a user-friendly, no-code interface, allowing teams to automate workflows, configure dashboards, and customize risk and compliance management without relying on extensive IT support.

Top Features

- → **Risk Cloud Quantify.** Enhances traditional risk assessment techniques with *Monte Carlo* simulations, enabling organizations to quantify risk in financial terms and connect it to business impact.
- → **Pre-Built Applications.** Provides over 20 pre-built applications tailored to specific GRC use cases, based on widely adopted standards and critical control frameworks.
- → **Third-Party Risk Management**. Includes applications to assess and manage third-party risks, helping organizations evaluate vendor performance and tighten security.

Advantages

→ **Advanced Visual Reporting.** Enables creation of distinctive visual reports with flexible customization of home screens and one-click report downloads [*].

→ **User-Friendly Customization.** Offers intuitive interface suitable for all technical levels, allowing real-time regulatory compliance without IT dependency [*].

→ **Unified Access Platform.** Provides single-pane-of-glass visibility with excellent implementation support and growing utilization potential [*].

→ **Integrated Security Overview.** Enables comprehensive end-to-end security program visibility with quantifiable metrics across multiple modules [*].

Disadvantages

→ **Limited Risk Analysis Data.** Absence of built-in loss data estimates requires manual customer input for risk analysis [*].

→ **Cost Concerns.** Full module set implementation can become expensive [*].

→ **Testing Environment Absence.** Lacks sandbox environment for testing changes before live implementation [*].

Pricing

→ Contact LogicGate Risk Cloud for more information.

11. Archer Insight

Archer Insight centralizes risk information and uses advanced analytics to provide real-time insights into risk exposure. The platform uses a combination of risk scoring, scenario modeling, and quantitative analysis to enable organizations to anticipate the potential impact of various risk events.

Archer Insight also includes tools for tracking risk tolerance and supporting the decision-making process, making it easier for organizations to align their risk strategies with business objectives.

The platform provides visibility into key risk indicators (KRIs) and integrates with incident management, compliance, audit, and business continuity tools within the broader Archer IRM suite. This enables organizations to build a comprehensive risk management program, monitor risk trends over time, and implement actionable strategies to optimize risk resilience.

Top Features

→ **Risk Quantification Methodology.** Offers a built-in quantitative risk assessment approach that replaces traditional qualitative methods, such as heat maps, with a series of straightforward questions. This methodology allows for the calculation of financial expected loss for quantitative risks.

→ **Archer Insight Workbench.** Provides a dedicated tool for risk modeling and analysis, enabling users to conduct in-depth evaluations of various risk scenarios and their potential impacts on the organization.

→ **Control Specification Assessment.** Allows for a detailed comparison of inherent, actual, and full states of a risk by specifying the control environment. This feature offers visibility into the effectiveness and value of each control in preventing risk occurrences or mitigating impacts.

→ **Quantitative Risk Aggregation.** Enables the aggregation of risk exposures across various hierarchy structures, such as assets, regions, divisions, and functions, providing a comprehensive view of enterprise-wide risk.

→ **Visualization of Risk Uncertainty**. Visualizes the full uncertainty around economic losses, leveraging common downside metrics like Value at Risk (VaR) and Conditional Value at Risk (CVaR). This visualization aids in understanding potential financial impacts under different risk scenarios.

→ **Risk Generator Application.** Allows users to quickly generate multiple risk records based on selected risk statements and target applications, streamlining the process of risk identification and documentation.

Advantages

→ **Comprehensive Vendor Governance.** Provides essential vendor risk management with methodical assessments, real-time monitoring, and customizable dashboards for quantified business risks [*].

→ **Customizable Workflow Management.** Enables full control over vendor risk management program development with customized workflows for stakeholders [*].

→ **Extensive Vendor Management.** Provides enterprise-wide management of vendor relationships, contacts, contracts, and risk exceptions with ongoing platform updates [*].

Disadvantages

→ **Cost and Update Issues.** High licensing costs combined with infrequent upgrades and limited automation capabilities [*].

→ **Resource-Intensive Customization.** Requires substantial resources including dedicated experts and consulting firms for custom dashboard creation and workflow implementation [*].

→ **Development Limitations.** Difficult to develop custom applications beyond out-of-box solutions, with complications in managing large-scale application structures [*].

→ **Browser Compatibility Issue.** Faces browser compatibility challenges requiring users to switch between different browsers, with poor user-friendliness requiring extensive customization [*].

Pricing

→ Contact Archer Insight for more information.

12. Fusion Framework

Fusion Framework System, developed by Fusion Risk Management, is a cloud-based operational resilience and risk management platform designed for business continuity, crisis management, and IT disaster recovery.

Developed by Fusion Risk Management, the solution provides real-time threat monitoring, automated incident response workflows, and integrated risk assessment capabilities.

Built on the Salesforce lightning platform, it offers a flexible and scalable solution for organizations looking for real-time threat monitoring, automated incident response workflows, and integrated risk assessment capabilities. This enables organizations to map dependencies between business services, processes, and IT assets while maintaining a centralized command center for incident management.

Fusion Framework System also supports mobile access for field response teams, provides geospatial risk visualization, and maintains audit trails for regulatory compliance across incident response activities.

Top Features

- **Dynamic Data Framework.** Allows organizations to create a tailored data model that reflects their unique operational structures and processes, ensuring that the system aligns with specific business needs.
- **Scenario Testing.** Enables users to simulate various disruption scenarios to evaluate potential impacts and the effectiveness of response strategies, thereby enhancing preparedness for unforeseen events.
- **Command Center.** Provides a centralized interface for real-time monitoring and management of incidents, facilitating swift and coordinated responses to emerging threats.
- **Dependency Mapping.** Provides a visual representation of relationships among people, processes, systems, and third parties, helping identify critical dependencies and potential points of failure.
- **Compliance Management.** Assists in tracking regulatory requirements, managing compliance activities, and maintaining audit trails to demonstrate adherence to relevant standards.

Advantages

- **Effective Compliance Management.** Provides clear compliance position visibility with robust access certification and control review capabilities [*].
- **Advanced Risk Analytics.** Delivers exceptional centralized risk data analysis with real-time dashboard capabilities for improved decision-making [*].
- **Comprehensive Coverage and Efficiency.** Fusion's extensive features cover all organizational needs from risk management to incident tracking, with adaptable dashboards that integrate well with business processes [*].

Disadvantages

- **1. Steep Learning Curve for New Users.** First-time users face overwhelming feature sets, requiring significant time to understand proper tool usage [*].
- **5. Performance Issues.** System experiences slowdowns during high-usage periods with delayed customer support responses [*].

→ **6. Processing Limitations.** Shows weak performance during heavy processing times, with feature complexity creating learning curve challenges for new users [*].

Pricing

→ Contact Fusion Risk Management for more information.

13. ServiceNow

ServiceNow GRC is an integrated risk and compliance management platform built on the ServiceNow digital workflow foundation.

The platform unifies operational, IT, and enterprise risk management through automated workflows, while leveraging AI capabilities for continuous monitoring and control testing.

The system provides real-time risk scoring, automated policy management, and compliance tracking across multiple frameworks (SOX, GDPR, NIST).

Its core features include continuous control monitoring, vendor risk management, and automated issue remediation with configurable SLAs and built-in audit trails. ServiceNow also maintains a single data model that connects risks, controls, and business processes.

Top Features

→ **Integrated Risk Management.** Provides a unified approach to identify, assess, and mitigate risks across the enterprise, ensuring alignment with business objectives.

→ **Policy and Compliance Management.** Centralizes the creation, management, and distribution of policies and standards, automating compliance workflows to ensure adherence to regulatory requirements.

→ **Audit Management.** Streamlines internal audit processes by automating audit planning, execution, and reporting, facilitating continuous monitoring and issue remediation.

→ **Third-Party Risk Management.** Assesses and monitors risks associated with third-party vendors, ensuring that external partnerships do not compromise organizational security and compliance.

→ **360° Relationship Visualization.** Offers a visual representation of relationships between different types of critical data, such as controls, risks, and issues.

Advantages

→ **Centralized Management Excellence.** Provides central management of risk, compliance, and governance processes with strong automation capabilities and real-time dashboard monitoring [*].

→ **ITIL Framework Integration.** Offers complete ITIL framework implementation with easy-to-use compliance-based ITSM solution that adapts quickly within organizations [*].

→ **Comprehensive Core Solution.** Delivers out-of-box functionality covering most process scenarios without requiring additional software deployment [*].

Disadvantages

- **Process Adaptation Challenges**. Requires significant upfront work to either adapt to ServiceNow's methodology or customize the platform to existing processes [*].
- **Implementation Constraints**. Requires additional vendor support for deployment, with limited flexibility in custom solutions and poor performing pre built components [*].
- **Template and UX Gaps**. Lacks sufficient starter templates with need for user experience improvements and modernization updates [*].

Pricing

- Contact ServiceNow for more information.

14. Enablon

Enablon by Wolters Kluwer is a comprehensive platform designed for EHS management, ESG reporting, risk assessment, and regulatory compliance. It offers real-time monitoring of operational risks and sustainability metrics, powered by automated data collection and analysis.

Key features include automated incident management, permit tracking, and emissions monitoring, with mobile access for field operations. Its ESG capabilities streamline sustainability reporting, carbon accounting, and environmental compliance, while ensuring audit trails for all activities.

The platform supports cloud and on-premises deployment, provides configurable workflows, and integrates with IoT devices for live environmental monitoring and safety alerts.

Top Features

- **ESG Excellence.** A solution that automates the collection of ESG data and integrates it into strategic business decisions and operations, facilitating comprehensive ESG reporting and performance management.
- **Process Safety Management.** Empowers organizations to implement effective process safety management by providing tools for engineers, managers, and field staff to enhance safety culture and operational reliability.
- **Health & Safety Management.** Offers a comprehensive solution to ensure the health and safety of workers, assets, and the wider community by managing and mitigating risks through integrated applications.
- **Enablon Juno.** An artificial intelligence (AI) component embedded within the platform's workflows, offering guidance, insights, and recommendations to users.
- **Open Insights.** A cloud-native analytics platform that empowers users to visualize and operationalize EHS, environmental, social, and governance (ESG), and integrated risk data, turning data into actionable insights.

Advantages

- **Essential Training Integration.** Provides vital onboarding tools for accident management, non-conformities, and quasi-incident handling as part of employee training [*].
- **Comprehensive EHS Management.** Delivers excellent environmental, health, and safety management capabilities with strong hazard evaluation and performance metric reporting [*].
- **Advanced Data Organization.** Offers advanced data organization with self-updating reports and graphics, enabling quick trend identification and analysis for non-expert users [*].

Disadvantages

- **User Proficiency Challenges.** Complex system logic requires extensive training for basic users, leading to a high number of queries about information access and data interpretation [*].
- **Programming Language Limitations.** Reliance on archaic NABSIC programming language creates coding difficulties and potential competitive disadvantages against newer solutions [*].
- **Limited User Interface Flexibility.** Lacks user-friendly features with restricted copy-paste functionality and limited customization options for forms and reports [*].

Pricing

- Contact Wolters Kluwer for more information.

15. LogicManager

LogicManager is a comprehensive Enterprise Risk Management (ERM) platform that integrates governance, risk management, and compliance activities into a centralized hub.

It uses taxonomy technology to connect risks across departments with controls, resources, processes, and personnel. This risk-based approach ensures proactive risk management while maintaining compliance through integrated monitoring and reporting capabilities.

LogicManager also provides role-based access controls, customizable assessment templates, and real-time reporting dashboards for stakeholder communication. In addition, it features a flexible architecture that supports various business functions through pre-built frameworks and configurable workflows.

Top Features

- **One-Click Compliance.** Reduces the effort and time required to satisfy compliance requirements by automating the mapping of controls to risks and compliance plans.
- **Integration Hub.** Offers a no-code, templated approach to connecting LogicManager with over 500 popular third-party applications.
- **Centralized Risk Libraries.** Offers pre-built, configurable libraries of industry-specific risks, controls, and assessment criteria, facilitating standardized data collection and risk assessments.

- → **Risk Maturity Model (RMM).** Promotes a two-way conversation with the board, risk committees, and risk officers. It provides benchmarking KPIs against industry standards, actionable steps to improve the risk program, and reporting ready to deliver to the board.
- → **Outcome-Based Advisory Services.** Offers dedicated advisory analysts who provide guided onboarding, support, and best-practice consulting. This partnership ensures that organizations receive the necessary guidance to achieve their risk management goals effectively.

Advantages

- → **Superior Customer Support.** Provides excellent support team assistance with powerful TPRM capabilities and effective SME workflow management [*].
- → **Centralized Vendor Management.** Delivers centralized vendor process management with no-code customization capabilities for real-time updates [*].
- → **Comprehensive Complaint Tracking.** Excels in complaint management with customizable fields and detailed reporting capabilities [*].

Disadvantages

- → **Licensing Cost Barriers.** User-based licensing model creates budget constraints for enterprise-wide deployment [*].
- → **Performance Issues.** Slow report generation, limited task notification customization, and insufficient data tracking capabilities [*].
- → **Limited Discussion Features in Assessments.** The absence of a feature for back-and-forth comments within risk and control self-assessments (RCSAs) limits detailed discussions, and the system's three-level risk and control scale restricts more granular analysis [*].

Pricing

- → Contact LogicManager for more information.

Implement an Effective Governance, Risk & Compliance Strategy — with ConductorOne

Every enterprise leader knows the delicate balance of GRC;

- → **staying compliant** without slowing down business,
- → **managing risk** without creating bottlenecks,
- → and **maintaining governance** without drowning in processes.

Your teams are juggling SOX compliance, wrestling with access certifications, and trying to prove to auditors that *'yes, you know exactly who has access to what and why.'*

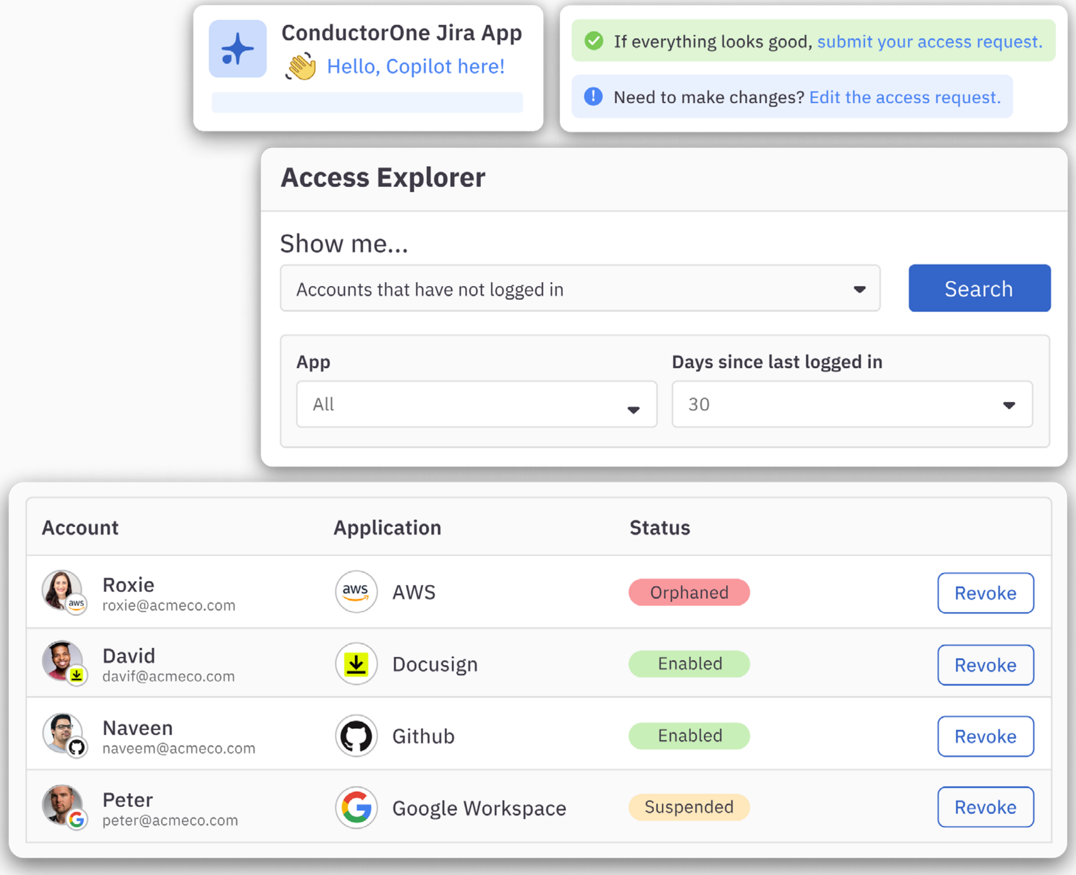
Meanwhile, your risk level keeps increasing with every new SaaS tool added to your stack, and your governance processes are struggling to keep pace with your company's growth.

Our friends at *Ramp*, a finance automation company, had similar issues. According to Paul Yoo, Ramp's Head of Security Assurance, —

> *"Different systems hold different types of data and in turn require different ways to secure access. Not everything works the same – you can't apply the same solution everywhere."*

Read Ramp's case study →

And that's why we built **CondutorOne**.



ConductorOne Jira App

👋 Hello, Copilot here!

✓ If everything looks good, submit your access request.

ⓘ Need to make changes? Edit the access request.

Access Explorer

Show me...

Accounts that have not logged in ▾ | Search

App	Days since last logged in
All ▾	30 ▾

Account	Application	Status	
Roxie roxie@acmeco.com	AWS	Orphaned	Revoke
David davif@acmeco.com	Docusign	Enabled	Revoke
Naveen naveem@acmeco.com	Github	Enabled	Revoke
Peter peter@acmeco.com	Google Workspace	Suspended	Revoke

We've automated the tedious parts of compliance, built intelligent risk detection that catches issues before they become problems, and created governance workflows that adapt to how your teams actually work.

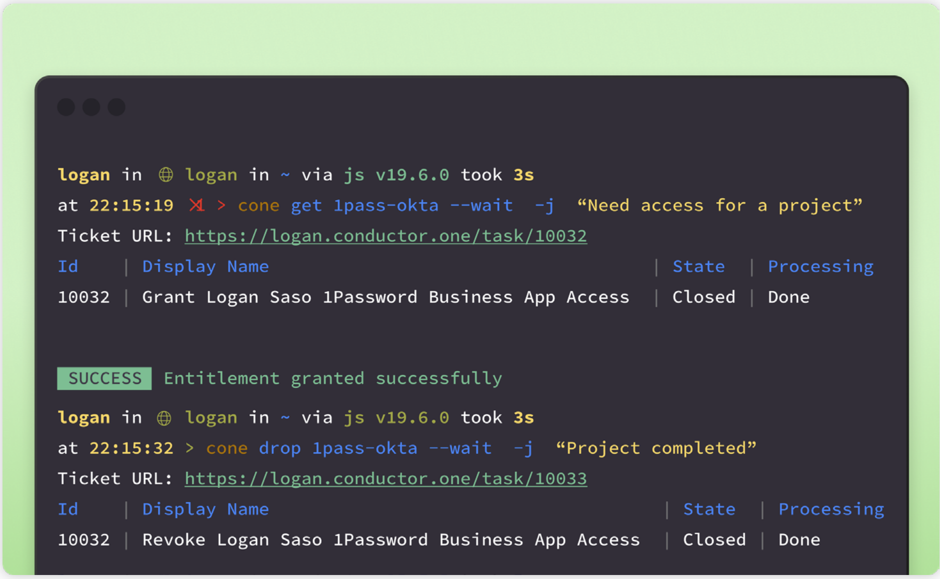
The result?

→ Your IT team spends less time on access reviews,

→ your security team gets clearer risk insights,

→ and your compliance team can pull audit reports in minutes, not weeks.

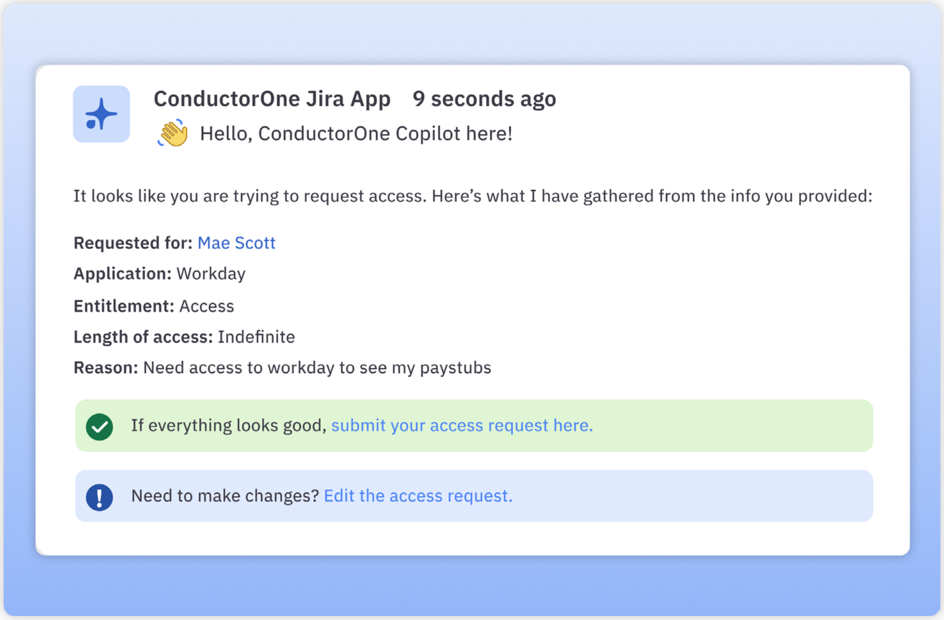
While most solutions force you to change your processes to fit their system, ConductorOne adapts to your existing workflows while making them better.



```
logan in 🌐 logan in ~ via js v19.6.0 took 3s
at 22:15:19 ✗1 > cone get 1pass-okta --wait  -j  “Need access for a project”
Ticket URL: https://logan.conductor.one/task/10032
Id    | Display Name                             | State  | Processing
10032 | Grant Logan Saso 1Password Business App Access  | Closed | Done


SUCCESS Entitlement granted successfully
logan in 🌐 logan in ~ via js v19.6.0 took 3s
at 22:15:32 > cone drop 1pass-okta --wait  -j  “Project completed”
Ticket URL: https://logan.conductor.one/task/10033
Id    | Display Name                              | State  | Processing
10032 | Revoke Logan Saso 1Password Business App Access  | Closed | Done
```

Our AI-powered platform learns your organization’s patterns and risk tolerance, automatically handling routine decisions and only escalating what truly needs attention.



ConductorOne Jira App **9 seconds ago**
👋 Hello, ConductorOne Copilot here!

It looks like you are trying to request access. Here’s what I have gathered from the info you provided:

Requested for: Mae Scott
Application: Workday
Entitlement: Access
Length of access: Indefinite
Reason: Need access to workday to see my paystubs

✓ If everything looks good, submit your access request here.

! Need to make changes? Edit the access request.

Whether you’re dealing with SOX, HIPAA, ISO 27001, or any other framework, we’ve designed our platform to make compliance feel less like a burden and more like a natural part of your business operations.

Audit Season Coming Up? → Let’s Get You Ready

Governance, Risk, & Compliance Tools (FAQs)

What Are GRC Tools?

GRC tools are specialized software solutions that help organizations manage governance, risk, and compliance activities in an organized, integrated manner.

These tools typically provide functionalities to:

→ **Risk Management.** Identify, evaluate, and mitigate risks within the organization.

→ **Compliance Management.** Automate compliance tasks, monitor regulatory changes, and ensure adherence to standards.

→ **Audit Management**. Facilitate audit planning, execution, and reporting processes.

→ **Incident Management.** Track and investigate incidents to resolve them effectively.

→ **Policy Management**. Centralize policy creation, dissemination, and attestation.

→ **Third-Party Risk Management.** Evaluate and monitor risks associated with vendors and external partners.

Who Typically Uses GRC Tools?

GRC tools are widely applicable across industries, as most organizations face regulatory requirements and risks.

However, they are particularly crucial in industries with strict regulations or high operational risks:

→ **Financial Services.** Banks, insurance companies, and investment firms use GRC tools to comply with strict financial regulations, manage transaction risks, and ensure data security.

→ **Healthcare.** Hospitals and healthcare providers leverage these tools to comply with patient privacy laws, maintain data security, and manage risks in clinical settings.

→ **Technology.** Tech firms use GRC tools to manage cyber risks, protect intellectual property, and comply with data privacy regulations.

→ **Manufacturing**. Manufacturing companies rely on GRC tools to meet safety standards, manage environmental compliance, and monitor supply chain risks.

→ **Government and Public Sector.** Public sector entities utilize GRC tools for regulatory compliance, transparency, accountability, and risk management in public services.

What Features Should You Look for in GRC Tools?

Key features to consider when evaluating GRC tools include:

→ **Risk Management.** Look for capabilities in risk identification, prioritization, and visualization (e.g., risk registers and heatmaps) and tools for monitoring Key Risk Indicators (KRIs).

→ **Compliance Management.** Essential features include regulatory tracking, policy and procedure management, compliance monitoring, and reporting functionalities.

→ **Incident Management.** Look for features that enable incident reporting, investigation, root cause analysis, and corrective action management.

What Are Common Challenges With GRC Implementation?

Implementing GRC solutions can be complex and may present challenges like:

→ **Data Silos.** Information often resides in separate systems across departments, making data integration difficult.

→ **Change Resistance.** Employees may resist adopting new processes or tools, which can slow down implementation.

→ **Cost and Complexity**. GRC programs require investments in technology and training, which can be resource-intensive.

→ **Regulatory Changes.** Constantly changing regulations demand agile, adaptable GRC processes to remain compliant.

→ **Executive Buy-in:** Without strong support from top management, GRC efforts may l ack the momentum and resources needed for success.

How Do Organizations Implement an Effective GRC Strategy?

To successfully implement a GRC strategy, organizations can follow these best practices:

→ **Define Clear Objectives.** Set specific goals for the GRC program aligned with overall organizational strategy.

→ **Secure Executive Support.** Gain buy-in from top management to ensure sustained support and resource allocation.

→ **Design an Integrated GRC Framework.** Integrate governance, risk, and compliance activities across the organization to provide a unified view.

→ **Select the Right Tools.** Choose GRC tools that align with your needs, streamline processes, and offer visibility into risk and compliance data.

→ **Promote a Compliance Culture.** Encourage a risk-aware culture by providing training and clear communication.

→ **Monitor Progress.** Track performance using key indicators to identify strengths and areas for improvement.

→ **Update Regularly.** Adjust the GRC strategy as regulations and business needs evolve.

Talk to our team.

Or take a self-guided tour to learn more!

Try ConductorOne now

Get a demo

AICPA SOC